



Hewlett Packard
Enterprise

HPE Security ArcSight ESM

Software Version: 6.11.0 Patch 2

Release Notes

April 27, 2018

Legal Notices

Warranty

The only warranties for Hewlett Packard Enterprise products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. Hewlett Packard Enterprise shall not be liable for technical or editorial errors or omissions contained herein.

The information contained herein is subject to change without notice.

The network information used in the examples in this document (including IP addresses and hostnames) is for illustration purposes only.

HPE Security ArcSight products are highly flexible and function as you configure them. The accessibility, integrity, and confidentiality of your data is your responsibility. Implement a comprehensive security strategy and follow good security practices.

This document is confidential.

Restricted Rights Legend

Confidential computer software. Valid license from Hewlett Packard Enterprise required for possession, use or copying. Consistent with FAR 12.211 and 12.212, Commercial Computer Software, Computer Software Documentation, and Technical Data for Commercial Items are licensed to the U.S. Government under vendor's standard commercial license.

Copyright Notice

© Copyright 2018 Hewlett Packard Enterprise Development, LP

Follow this link to see a complete statement of copyrights and acknowledgements:

<https://community.softwaregrp.com/t5/Discussions/Third-Party-Copyright-Notices-and-License-Terms/td-p/1589228>

Support

Contact Information

Phone	A list of phone numbers is available on the Technical Support Page: https://softwaresupport.softwaregrp.com/support-contact-information
Support Web Site	https://softwaresupport.softwaregrp.com/
ArcSight Product Documentation	https://community.softwaregrp.com/t5/ArcSight-Product-Documentation/ctp/productdocs

Contents

Welcome to ESM 6.11.0 Patch 2	5
Important Prerequisite: Must Have Spectre and Meltdown Patches Applied	5
Purpose of this Patch	5
Upgrade Support	5
Vulnerability Updates	6
Geographical Information Update	6
Usage Notes	6
Uninstalling the Console Patch on the Mac	6
Cannot Install ArcSight Console Patch for Mac Operating System into /current Directory	7
Authentication Between IE 11 and PKCS#11 Token	7
Correction to the Formula for Correlation Data Monitor	7
Variables on the ArcSight Command Center	8
Reference to SmartConnectors Not Updated (Customer URI)	9
SSL Client Authentication Not Available After Adding 6.11.0 Patch	9
Silent Install is not Supported in Dark Theme for ESM 6.11.0	9
Audit Events Now Generated by Creation or Deletion of Mark Similar Configurations	10
Section 508 Compliance	10
Installing ESM Version 6.11.0 Patch 2	10
Verifying the Downloaded Installation Software	11
If You Have the B7500 (G8) Appliance on RHEL 6.8 or RHEL 7.3	11
ArcSight ESM Main Component Suite	12
To Install the Patch	12
After Patch Installation: RHEL 7.2 and 7.3 and CentOS 7.3	14
To Uninstall the Patch	14
ArcSight Console	15
To Install the Patch	15
To Install the Patch on a Mac	17
To Uninstall the Patch	18
Fixed Issues	19
Analytics	19
ArcSight Console	20
ArcSight Manager	22
CORR-Engine	23
Command Center	24

Connectors	24
General	24
Installation and Upgrade	24
Open Issues	25
Command Center	25
Open and Closed Issues in ESM 6.11.0 Patch 1	25
Send Documentation Feedback	26

Welcome to ESM 6.11.0 Patch 2

ArcSight Enterprise Security Management (ESM) is a comprehensive software solution that combines traditional security event monitoring with network intelligence, context correlation, anomaly detection, historical analysis tools, and automated remediation. ESM is a multi-level solution that provides tools for network security analysts, system administrators, and business users.

ESM includes the Correlation Optimized Retention and Retrieval (CORR) Engine, a proprietary data storage and retrieval framework that receives and processes events at high rates, and performs high-speed searches.

Important Prerequisite: Must Have Spectre and Meltdown Patches Applied

As a prerequisite to installing ESM 6.11.0 Patch 2, you must have the patches for the Spectre and Meltdown vulnerabilities applied to your operating system.

Purpose of this Patch

This patch:

- Updates the JRE to 1.8.0_161-b11
- Addresses critical issues in ESM 6.11.0.
- Provides updates for geographical information and vulnerability mapping.
- Provides important security updates.
- Audit events are now generated by the creation or deletion of mark similar configurations. See "[Audit Events Now Generated by Creation or Deletion of Mark Similar Configurations](#)" on page 10 for details.

Refer to the [ArcSight ESM Support Matrix](#) for the new and existing operating systems supported in this patch.

Upgrade Support

Apply this patch on ESM 6.11.0, with or without a released patch.

If you have older versions of ESM, upgrade those versions to 6.11.0 first before applying this patch.

For details on supported platforms, refer to the *ESM Support Matrix* available from the [Protect724 Community](#).

Vulnerability Updates

This release includes recent vulnerability mappings from the April 2018 Context Update.

Device	Vulnerability Updates
Snort / Sourcefire SEU 2983 updated	Bugtraq, X-Force, MSSB, Faultline, CVE, Nessus, CERT
Enterasys Dragon IDS updated	CVE
Cisco Secure IDS S1016 updated	CVE
Juniper IDP update 3053 updated	Bugtraq, X-Force, MSSB, Faultline, CVE, Nessus, CERT, MSKB
McAfee Intrushield updated	Bugtraq, X-Force, MSSB, Faultline, CVE, Nessus
TippingPoint UnityOne DV9086 updated	Bugtraq, MSSB
McAfee HIPS 7.0 updated	CVE

Geographical Information Update

This version of ESM includes an update to the geographical information used in graphic displays. The version is GeoLite2-City_20180401.

Usage Notes

Uninstalling the Console Patch on the Mac

When uninstalling the Console Patch on the Mac, if the uninstall binary (Uninstall_ArcSight_ESM_Console_Patch) located in <CONSOLE_HOME>/current/UninstallerData_6.11.0.2 is used to uninstall the patch, then the UninstallerData_6.11.0.2 directory is not deleted and the presence of this directory prevents reinstallation after the uninstall is done.

Workaround:

Use the symbolic link created when the patch was installed to invoke the Console Patch Uninstaller on the Mac, instead of the uninstall binary located in <CONSOLE_HOME>/current/UninstallerData_6.11.0.2. After deleting this directory, you can re-install the ArcSight Console ESM patch.

Cannot Install ArcSight Console Patch for Mac Operating System into /current Directory

An error occurs if you attempt to install the patch into the default /current directory on the Mac operating system. Instead, install into the root folder of the existing ESM 6.11.0 installation (for example, /Applications/arcsight_611_GA).

Authentication Between IE 11 and PKCS#11 Token

When using Internet Explorer 11 with ActivClient middleware and a PKCS#11 token, an error is displayed:

This page can't be displayed

This prevents the user from logging into ArcSight Command Center.

If there are problems with the PIN dialog to log into the card in some client (Firefox, IE, Chrome, ArcSight Console), try another client. Once the card is successfully authenticated through that client, the middleware (for example ActivClient) might skip card authentication, when you repeat PKCS#11 login from the original client.

Correction to the Formula for Correlation Data Monitor

The ArcSight Console Guide has a topic, "Event Correlation Data Monitor." The formula is not correct. This usage note provides the correct formulas and explains how these formulas are used in the data monitor.

How correlation is calculated

The event correlation data monitor applies covariance and correlation calculations to describe how two variables are related.

Covariance is calculated by the following formula:

$$COV(x,y) = \frac{\sum_{i=1}^n (x_i - \bar{x})(y_i - \bar{y})}{n - 1}$$

where:

x is the independent variable

y is the dependent variable

\bar{x} is the mean of the independent variable x

\bar{y} is the mean of the dependent variable y

Based on the covariance, correlation is then calculated by the following formula:

$$r(x, y) = \frac{COV(x, y)}{s_x s_y}$$

where:

$r(x, y)$ is the correlation of variables x and y

$COV(x, y)$ is the covariance of variables x and y

s_x is the sample standard deviation of the random variable x

s_y is the sample standard deviation of the random variable y

Correlation standardizes the measure of interdependence between two variables and, consequently, tells you how closely the two variables move. The correlation measurement, called a correlation coefficient, will always take on a value between 1 and -1:

- *If the correlation coefficient is 1*, the variables have a perfect positive correlation. This means that if one variable moves a given amount, the second moves proportionally in the same direction. A positive correlation coefficient less than one indicates a less than perfect positive correlation, with the strength of the correlation growing as the number approaches one.
- *If correlation coefficient is 0*, no relationship exists between the variables. If one variable moves, you can make no predictions about the movement of the other variable; they are uncorrelated.
- *If correlation coefficient is -1*, the variables are perfectly negatively correlated (or inversely correlated) and move in opposition to each other. If one variable increases, the other variable decreases proportionally. A negative correlation coefficient greater than -1 indicates a less than perfect negative correlation, with the strength of the correlation growing as the number approaches -1.

The data monitor sampler takes all samples in memory and continually calculates correlation values using this formula. As an example, you could define an event correlation data monitor that displays a correlation between the number of times a network is being reconnoitered, and if that is related to the number of attacks that the network is receiving.

Variables on the ArcSight Command Center

The ArcSight Command Center does not support global and local variables. The ArcSight Command Center supports only standard event fields for viewing. Variables (global or local) are not supported. Use the ArcSight Console instead. See the following table:

Fields

User Interface	Standard Event Fields	Local Variables	Global Variables
ArcSight Command Center	Yes	No	No
ArcSight Console	Yes	Yes	Yes

Reference to SmartConnectors Not Updated (Customer URI)

When the customer object is renamed on the ArcSight Console, the associated reference to SmartConnectors (the Customer URI) is not updated with the new name. The Customer URI on the connector retains the old name. This is expected behavior and not an issue.

SSL Client Authentication Not Available After Adding 6.11.0 Patch

After applying 6.11.0 Patch 2, the ArcSight Console in the Default-SSL console client does not connect to the Manager. The issue is that the Manager certificate is not in the client ArcSight Console truststore.

Workaround:

Copy `jre.pre6.11.0.2\lib\security\cacerts` `jre\lib\security\cacerts`

Silent Install is not Supported in Dark Theme for ESM 6.11.0

When in silent mode, the ESM Console installer does not trigger the `consolesetup` step at the end of the install. As a result, a default `console.properties` file is not generated during the installation. Dark theme requires access to this properties file.

Workaround:

1. Run the `consolesetup` wizard in first in recording mode to capture a silent response file. For example:

```
arcsight consolesetup -i recorderui -f console_silent.out
```
2. Use the response file `console_silent.out` to run `consolesetup` in silent mode. For example:

```
arcsight consolesetup -i silent -f <full path to console_silent.out>
```

This results in a `config/console.properties` file in the ESM Console installation.
3. Now use the dark theme.

Syntax:

Note that the `consolesetup` command supports the following parameters:

`consolesetup [-i <mode>] [-f <file>] [-g]`

Parameters :

-i <mode> (modes are: console, silent, recorderui, swing)

-f <file> Log file name (properties file in -i silent mode)

-g (generate sample properties file for -i silent mode)

See the *ESM Administrator's Guide*, Appendix A: Administrative Commands for details on commands and parameters.

Audit Events Now Generated by Creation or Deletion of Mark Similar Configurations

The creation or deletion of mark similar configurations now generates audit events.

ID	Message	Priority
marksimilar:102	Mark similar configuration created Low	Low
marksimilar:100	Mark similar configuration removed due to time window expiry	Low
marksimilar:100	Mark similar configuration removed due to error. Check server.log	High
marksimilar:100	Mark similar - all have been removed	Medium

Section 508 Compliance

ArcSight recognizes the importance of accessibility as a product initiative. To that end, ArcSight continues to make advances in the area of accessibility in its product lines.

Installing ESM Version 6.11.0 Patch 2

You can install this patch release using the platform-specific component executable files provided. Patch installers are available for all supported platforms.

Note: Keep the following points in mind when installing Patch 2:

- As a prerequisite to installing ESM 6.11.0 Patch 2, you **must** have patches for the Spectre and Meltdown vulnerabilities applied to your operating system.
- **For all components and platforms:** Make sure that you have enough space available *before* you install the patch. The installer checks for 1 GB of space and generates an error if it is not available. If you run into disk space issues during installation, create enough space, restore the component base build from the backup, then resume patch installation.
- Backup, patch install, and uninstall procedures require permissions for the relevant components. To install a patch, make sure that the user who owns the base build installation folder has full privileges on the PATH where the base build is installed.
- To uninstall the software you must be at the same user level as the original installer.
- It is a good practice to create a backup of the existing product before installation begins. Do not simply rename files and leave them in the same directory. Java reads all the files present, regardless of renaming, and can pick up old code inadvertently, causing undesirable results.
- For backup, patch install, and uninstall, we recommend that you log in to the target machine with a specific account name using SSH. If you switch accounts after logging in, then specify the flag `"-"` for the **su** command (`su - <UserName>`).

Each component has install and uninstall steps.

Caution: Do not interrupt the patch install process (for example, do not press Ctrl-C or log off). Interrupting the process would cause issues.

Verifying the Downloaded Installation Software

HPE provides a digital public key to enable you to verify that the signed software you received is indeed from HPE and has not been manipulated in any way by a third party.

Visit the following site for information and instructions:

<https://h22253.www2.hpe.com/ecommerce/efulfillment/digitalSignIn.do>

If You Have the B7500 (G8) Appliance on RHEL 6.8 or RHEL 7.3

If you are upgrading from ESM 6.11.0 to 6.11.0 Patch 2 on a B7500 (G8) appliance with RHEL 6.8 and you do not want to upgrade the OS to RHEL 6.9, you must first install the standalone tzdata updater. Otherwise, the ESM 6.11.0 Patch 2 installer will display an error stating that you have an out-of-date tzdata package.

Note: If you are on RHEL 6.8, we recommend that you update to RHEL 6.9 before applying the

patch. RHEL contains security fixes.

Upgrade to RHEL 7.4 is not supported on the B7500 (G8) appliance.

The standalone tzdata updater is *not* required if you have one of these configurations:

- ESM, software version
- ESM Express (G9) that has been upgraded to RHEL 7.4.
- ArcSight Express (G8) that has been upgraded to RHEL 6.9

To install the tzdata updater on the B7500 appliance:

1. Log in as **root**.
2. Go to the HPE Software download site (<http://softwaresupport.hpe.com>)
3. Download the package `esm_tz_standalone_2017c.tar.gz` to a directory of choice on the appliance. In this example, we will use `/opt/upgrades`.

4. Go to `/opt/upgrades` and extract the archive with this command:

```
tar -xzf esm_tz_standalone_2017c.tar.gz
```

where `esm_tz_standalone_2017c` is a directory you designate.

5. Go to the new `<bundle_name>` directory, using our example:

```
cd /opt/upgrades/esm_tz_standalone_2017c
```

6. Run this command:

```
./tz_patch.sh
```

Wait for the message that confirms a successful update. In case of failures, the message will inform the reason, for example, unsupported platform or non-root user.

You can now proceed to the ESM 6.11.0 Patch 2 installation.

ArcSight ESM Main Component Suite

This section describes how to install or uninstall the ESM 6.11.0 Patch 2 for all the main components except the ArcSight Console. These components include the Manager and the CORR-Engine.

To Install the Patch

Note: Installation considerations:

- Before you install the patch, verify that `<ARCSIGHT_HOME>` and any of its subdirectories are not being accessed by open shells on your system.
- If for any reason you need to re-install the patch, follow the steps in the subsection "To Uninstall the Patch" later in this section before installing the patch again.

- It is recommended that you continue through the installation and do not attempt to cancel the installation process or move backward through the installer windows.

1. Download the patch from the software download site (<http://softwaresupport.hpe.com>).

ArcSightESMSuitePatch-XXXX.tar

...where XXXX represents the suite build number.

Be sure to verify the patch file; see "[Verifying the Downloaded Installation Software](#)" on page 11.

2. As user *arcsight*, extract the tar file.

3. Stop the ArcSight services as user *arcsight*:

```
service arcsight_services stop all
```

4. Back up the ArcSight directory, `/opt/arcsight`, by making a copy. Place the copy in a readily accessible location. This is a precautionary measure so you can restore the system to the original state, if necessary.

Caution: HPE recommends that you do not simply rename files and leave them in the same directory. Java reads all the files present, regardless of renaming, and can pick up old code inadvertently, causing undesirable results.

5. If you have High Availability configured, run the following command on the secondary server as user *root* to put the server in standby mode:

```
crm_standby -v true
```

6. From the directory where you extracted the tar file, run the patch installer as user *arcsight*:

```
./ArcSightESMSuitePatch.bin
```

To install in Console mode, run the following command from the shell prompt and then follow the instructions in the window:

```
./ArcSightESMSuitePatch.bin -i console
```

7. Read through the license agreement and accept it at the end. In GUI mode, the acceptance check box is disabled until you scroll to the bottom of the agreement. In console mode, press the **Enter** key until you have paged through to the end of the license agreement.
8. Select a location for the uninstaller link, if you want to have a shortcut to the uninstaller in some other location. You must have write permission to the specified folder.
9. Check the pre-installation summary to verify that all the locations listed are correct and that you have enough disk space to install this patch.
10. Press **Enter** to start the installation.
11. When the installation is complete press **Enter** to Exit.

Note: If you upgraded from 6.9.1c to 6.11.0, did you configure SSL Client Authentication using `keytoolgui` to generate keypairs and certificates?

If so, after completing patch installation at this step and before restarting services, regenerate the certificates.

12. Start the ArcSight services as user *arcsight*:

```
service arcsight_services start all
```

13. If you have High Availability configured, run the following command on the secondary server as user *root* to bring the server online:

```
crm_standby -D
```

After Patch Installation: RHEL 7.2 and 7.3 and CentOS 7.3

After applying the patch, if the `postgresql` service becomes unavailable, check this log file:

```
/opt/arcsight/logger/userdata/logs/pgsql/serverlog
```

for the following messages:

```
FATAL: semctl(2162718, 14, SETVAL, 0) failed: Invalid argument
```

```
FATAL: sorry, too many clients already
```

If you see these FATAL messages, perform the following steps:

1. As user **root**, edit the file `/etc/systemd/logind.conf`.
2. Search for `RemoveIPC`, and ensure there is only one instance of this property.
3. Edit the property if it exists (or add the property if it does not exist) to have the value **no**:

RemoveIPC=no

4. Run this command:

```
systemctl restart systemd-logind.service
```

To Uninstall the Patch

If needed, use the procedure below to uninstall this patch installation and restore the system to the pre-patched state.

Note: Before you begin to uninstall, verify that the Manager's `<ARCSIGHT_HOME>` and any of its subdirectories are not being accessed by any open shells on your system.

1. Stop the ArcSight services as user *arcsight*:

```
service arcsight_services stop all
```

2. If you have High Availability configured, run the following command on the secondary server as

user *root* to put the server in standby mode:

```
crm_standby -v true
```

3. As user *arcsight*, run the uninstaller program from either the directory where you created the link while installing the product or, if you had opted not to create a link, then run this from the `/opt/arcsight/suitepatch_6.11.0.2/UninstallerData_6.11.0.2` directory:

```
./Uninstall_ArcSight_ESM_Suite_Patch
```

Alternatively, you can run the following command from the `/home/arcsight` (or wherever you installed the shortcut link) directory:

```
./Uninstall_ArcSight_ESM_Suite_Patch_6.11.0.2
```

Or, to uninstall using Console mode, run:

```
./Uninstall_ArcSight_ESM_Suite_Patch_6.11.0.2 -i console
```

Run the uninstaller in the same mode in which you ran the installer (GUI or Console mode).

4. When the uninstallation is complete press **Enter** to Exit.

5. Start the ArcSight services as user *arcsight*:

```
service arcsight_services start all
```

6. If you have High Availability configured, run the following command on the secondary server as user *root* to bring the server online:

```
crm_standby -D
```

ArcSight Console

This section describes how to install or uninstall the ESM 6.11.0 Patch 2 for ArcSight Console on Windows, Mac, and Linux platforms.

Tip: The ArcSight ESM Console is not supported on AIX or Solaris. The following steps do not include information for installing a Console patch on those platforms.

To Install the Patch

Note: Installation considerations:

- Before you install the patch, verify that the Console's `<ARCSIGHT_HOME>` directory and any of its subdirectories are not being accessed by any open shells on your system.
- If you need to re-install the patch, run the patch uninstaller before installing the patch again.
- It is recommended that you continue through the installation and do not attempt to cancel the installation process or move backward through the installer windows.

1. Exit the ArcSight Console.
2. Back up the Console directory (for example, /home/arcsight/console/current) by making a copy. Place the copy in a readily accessible location. This is a precautionary measure so you can restore the original state, if necessary.

Caution: It is recommended that you do not simply rename files and leave them in the same directory. Java reads all the files present, regardless of renaming, and can pick up old code inadvertently, causing undesirable results.

3. Download the executable file specific to your platform from the Software Support Online site (<http://softwaresupport.hpe.com>). YYYY.Y represents the Console build number.
 - Patch-6.11.0.YYYY.Y-Console-Win.exe
 - Patch-6.11.0.YYYY.Y-Console-Linux.bin
 - Patch-6.11.0.YYYY.Y-Console-MacOSX.zipBe sure to verify the patch file; see "Verifying the Downloaded Installation Software" on page 11.
For the Mac, see "To Install the Patch on a Mac" on the next page.
4. Run one of the following executables specific to your platform:
 - **On Windows:**
Double-click Patch-6.11.0.YYYY.Y-Console-Win.exe
 - **On Linux:**
Verify that you are logged in as user *arcsight*, and then run the following command:

```
./Patch-6.11.0.YYYY.Y-Console-Linux.bin
```


To install in Console mode, run the following command from the shell prompt and then follow the instructions in the window:

```
./Patch-6.11.0.YYYY.Y-Console-Linux.bin -i console
```


The installer launches the Introduction window.
5. Read the instructions provided and Press **Enter**.
6. Accept the terms of the license agreement and press **Enter**. In GUI mode the acceptance check box is disabled until you scroll to the bottom of the agreement. In Console mode, press **Enter** until you have read every page, and then Press **Enter** to accept the agreement.
7. Select the location of your existing <ARCSIGHT_HOME> directory for your Console installation by typing the appropriate choice and pressing **Enter**
If you want to restore the installer-provided default location, select **Restore Default Folder**.
8. Press **Enter** to continue.
9. Select a Link Location (on Linux) or Shortcut location (on Windows) by clicking the appropriate check box and Press **Enter** or click **Next**.

10. Check the pre-installation summary to verify that all the locations listed are correct and that you have enough disk space to install this patch.
11. Press **Enter** to start the installation.
12. When the installation is complete, press **Enter** to exit.

Note: If you upgraded from 6.9.1c to 6.11.0, did you configure SSL Client Authentication using `keytoolgui` to generate keypairs and certificates?

If so, after completing patch installation at this step and before restarting services, regenerate the certificates.

To Install the Patch on a Mac

The patch installer download and run procedure is slightly different on the Mac than on the other supported platforms. See the Usage Note ["Cannot Install ArcSight Console Patch for Mac Operating System into /current Directory" on page 7](#) for details.

Note: It is recommended that you continue through the installation and do not attempt to cancel the installation process or move backward through the installer windows.

1. Exit the ArcSight Console.
2. Back up the Console directory (for example, `/home/arcsight/console/current`) by making a copy. Place the copy in a readily accessible location. This is just a precautionary measure so you can restore the original state, if necessary.
3. Download the file `Patch-6.11.0.YYYY.Y-Console-MacOSX.zip` to anywhere on your system.

Tip: The patch installer file shows as a **ZIP** file on the download site, but downloads as `ArcSightConsolePatch.app` on the Mac. A single or double-click on this **APP** file launches the patch installer, depending on how you have set these options. There is no need to “extract” or “unzip” the file; it downloads as an **APP** file.

Be sure to verify the patch file; see ["Verifying the Downloaded Installation Software" on page 11](#).

4. Launch the patch installer by double-clicking the `ArcSightConsolePatch` file.
5. Follow the steps on the patch install wizard, providing the information as prompted:
 - Accept the terms of the license agreement and click **Next**. The acceptance check box is disabled until you scroll to the bottom of the agreement.
 - Choose the location where you want to install the patch. Browse to `<ARCSIGHT_HOME>`, where your previous Console was installed.
 - Choose an alias location for the Console application (or opt to not use aliases). This is the same as a link location on UNIX systems or shortcut location on Windows systems.

6. Click **Next**.
7. Verify your settings and click **Install**.

Note: If you upgraded from 6.9.1c to 6.11.0, did you configure SSL Client Authentication using `keytoolgui` to generate keypairs and certificates?

If so, after completing patch installation at this step and before restarting services, regenerate the certificates.

To Uninstall the Patch

If needed, use the procedure below to uninstall this patch installation.

Note: Before you begin to uninstall, verify that the Console's <ARCSIGHT_HOME> and any of its subdirectories are not being accessed by any open shells on your system.

1. Exit the ArcSight Console.
2. Run the uninstaller program:

On Windows:

- Double-click the icon you created for the uninstaller when installing the Console. For example, if you created an uninstaller icon on your desktop, double-click that icon.
- If you created a link in the Start menu, click:

Start > All Programs > ArcSight ESM Console 6.11.0 Patch 2 > Uninstall ArcSight ESM Console 6.11.0 Patch 2

- Or, run the following from the Console's <ARCSIGHT_HOME>\current\UninstallerData_6.11.0.2 directory:

`Uninstall_ArcSight_ESM_Console_Patch.exe`

- **On Linux:**

- From the directory where you created the link when installing the Console (your home directory or some other location), run:

`./Uninstall_ArcSight_ESM_Console_Patch_6.11.0.2`

- Or, to uninstall using Console mode, run:

`./Uninstall_ArcSight_ESM_Console_Patch_6.11.0.2 -i console`

- If you did not create a link, execute the command from the Console's <ARCSIGHT_HOME>/current/UninstallerData_6.11.0.2 directory:

`./Uninstall_ArcSight_ESM_Console_Patch`

- Or, to uninstall using Console mode, run:

```
./Uninstall_ArcSight_ESM_Console_Patch -i console
```

On a Mac:

- From the directory where you created the link when installing the Console, run:

```
Uninstall_ArcSight_ESM_Console_Patch_6.11.0.2
```

- From the Console's <ARCSIGHT_HOME>/current/UninstallerData_6.11.0.2 directory, run:

```
Uninstall_ArcSight_ESM_Console_Patch
```

3. Click **Done** on the Uninstall Complete screen.

Note: If you are on a Windows system and you plan to uninstall the base build Console after uninstalling Patch 2, be advised that your system restarts without warning upon finishing the base build uninstallation. Prepare your system accordingly.

Fixed Issues

The following issues are fixed in this release.

• Analytics	19
• ArcSight Console	20
• ArcSight Manager	22
• CORR-Engine	23
• Command Center	24
• Connectors	24
• General	24
• Installation and Upgrade	24

Analytics

Issue	Description
NGS-22829	Error messages related to inconsistencies with buckets have been changed to [INFO].
NGS-19673	Active channels using filters or field sets that had a local variable with the function Get active list value were not populating this variable correctly. This issue has now been fixed and GetActiveListValue works as expected.

Issue	Description
NGS-13974	Reports which output the URL filename will no longer suppress the leading slash (/). This will match the ArcSight Console output. So, the filename portion of the URL <code>http://www.google.com/index.html</code> is <code>/index.html</code> . URL <code>http://www.google.com/</code> will be <code>/</code> and URL <code>http://www.google.com</code> is <code>NULL</code> .

ArcSight Console

Issue	Description
NGS-27231	<p>The property <code>console.ui.channel.disable.sorting</code> has been extended to prevent sorting Active Channels on any fields other than End Time or Manager Receipt Time, by hot key combination of CTRL+CLICK on the column headers.</p> <p>Note, that on the MacOS, the CTRL+CLICK operation triggers the same context menu as a RIGHT-CLICK operation. This specific MacOS behavior will not be affected and the CTRL+CLICK on the table header will still present the header item's context menu.</p>
NGS-27211	When the customer object is renamed on the ArcSight Console, the associated reference to SmartConnectors (the Customer URI) is not updated with the new name. The Customer URI on the connector retains the old name. This is expected behavior and not an issue.
NGS-27186	<p>The creation or deletion of mark similar configurations now generates audit events.</p> <p>ID Message Priority</p> <p>marksimilar:102 Mark similar configuration created Low</p> <p>marksimilar:100 Mark similar configuration removed due to time window expiry Low</p> <p>marksimilar:100 Mark similar configuration removed due to error. Check server.log High</p> <p>marksimilar:100 Mark similar all have been removed Medium</p>
NGS-26834	An Active List import did not to upload documents with more than 512 characters. The fix was to change the length max to 999 characters, enabling long string import.
NGS-26696	Annotating events with Mark Similar does not enforce required fields like User and Comment. If User and Comment are enforced after Mark as Similar set, then the Mark As Similar Config will be removed since the User and Comment fields are now enforced. If the Mark as Similar is set after User and Comment are set required on stage, then the Mark As Similar dialog will force user to set the User and Comment fields.
NGS-26644	<p>When editing stages, the "mark similar stage" option could only be edited when the "mark similar flag" was checked. Users, sometimes, wished to "mark similar stage" but did not check the flag.</p> <p>The mark similar stage is now editable.</p>
NGS-26639	<p>The change of the Field Set used by a Rule Action has caused the loss of previous event values.</p> <p>This issue has been fixed.</p>
NGS-26431	<p>The static banner background color at the top of the console was not displaying properly.</p> <p>This issue has been fixed.</p>

Issue	Description
NGS-25966	<p>To suppress pop-up messages and dialogs during brief ESM subsystem outages, the following flag can be added to console.properties:</p> <pre>generalSystemPopups.suppress=true</pre> <p>When this flag is set to true, the ArcSight Console will not show pop-up messages or dialogs relating to the subsystem outage. However, the messages will still be logged on the ArcSight Console's bottom status bar, and can be viewed at any time by clicking on that status bar.</p>
NGS-25886	<p>The Event Inspector Table, when viewed in the console, was taking a large portion of the CPU even when the user was idle. This affected all operating system platforms, but was more of an issue on the Macbook MacOS platforms.</p> <p>This issue has been fixed.</p>
NGS-25617	<p>There is an issue with the ESM Console installer when run in silent mode. In this case, the installer does not trigger the consolesetup step at the end of the install. The result of this skipped step is that a default console.properties file is not generated during the installation. The missing console.properties causes the issue when attempting to apply the dark theme, which requires access to this properties file.</p> <p>Workaround:</p> <p>Run the consolesetup wizard in silent mode, which is supported and documented in the ESM Administrator's Guide, Appendix A: Administrative Commands. Run consolesetup first in recording mode to capture a silent response file. For example:</p> <pre>arcsight consolesetup -i recorderui -f console_silent.out</pre> <p>Then, use this response file to run consolesetup in silent mode. For example:</p> <pre>arcsight consolesetup -i silent -f <full path to console_silent.out></pre> <p>This should result in a config/console.properties" file in the ESM Console installation.</p> <p>The consolesetup command supports the following parameters:</p> <p>Syntax consolesetup [-i <mode>] [-f <file>] [-g]</p> <p>Parameters -i <mode> Mode: console, silent, recorderui, swing</p> <p>-f <file> Log file name (properties file in -i silent mode)</p> <p>-g Generate sample properties file for -i silent mode</p>
NGS-24664	<p>Previously, ESM had a restriction on ArcSight Console logins from hosts with certain fully qualified domain names. That restriction has been removed.</p>
NGS-23987	<p>A change was made that resulted in the possibility of negative values for Entry Expiration Times (EET), which were not handled correctly by the Use Case Wizard EET panel.</p> <p>The Use Case Wizard EET panel and Session List editor now support zero values and negative (for legacy negative values) as Unlimited.</p>
NGS-22284	<p>The action Move to another network resulted in a pop-up for each Zone processed. The behavior has been changed so that all Zones will be processed and then a single result message displayed, with additional details available in the console.log if needed</p>
NGS-10348	<p>The new boolean property query.dateformat.iso8601 was added to server.properties. Set it to true to retrieve week values in an ISO 8601 compliant format for queries and reports.</p>

ArcSight Manager

Issue	Description
NGS-27140	<p>New stages cannot mark similar and existing stages, and so could have the wrong mark on a similar stage even if require mark similar is checked. This can cause the wrong stage to be set on mark similar for subsequent events.</p> <p>Workaround:</p> <p>To fix any stage with this issue, save the stage again in the ArcSight Console.</p>
NGS-27082	<p>Mark similar stage changes could throw errors that break channel event flow due to stages having incompatible flags. e.g.require user or comment.</p> <p>Mark similar configuration that throw errors are now removed to avoid breaking the event flow. A channel to monitor mark similar configurations can be created with the filter: name StartsWith "Mark similar".</p>
NGS-26900	<p>Bad custom mark similar filters could break the event due to parsing errors.</p> <p>Mark similar configurations with bad filters are now being removed, and an error is displayed, indicating the filter should be corrected.</p>
NGS-26472	<p>The Manager does not display or store custom zones correctly when aggregation is enabled.</p> <p>This issue has been fixed. Now as long as the Preserve Common Fields is set to yes, the aggregated events will have custom zone information.</p>
NGS-26267	<p>Upgrade to RADIUS third party library broke capability to fail over to secondary server.</p> <p>This issue has been fixed.</p>
NGS-25443	<p>The Rest API call, findByUUID, was failing in ESM 6.11.0. This issue has been fixed, and the REST API behavior should now be consistent with earlier ESM versions.</p>
NGS-25388	<p>Rule parsing exceptions could occur due to update of velocity libraries in ESM 6.11.0, preventing the Manager from starting.</p> <p>This issue has been fixed.</p>
NGS-24963	<p>Asset auto-creation did not work due to a mismatch in default URIs.</p> <p>This issue has been fixed.</p>
NGS-24944	<p>Log messages related to Logger and not related to an event searcher are now at the debug level. To reenable them, set the Logger property log.global.debug in the logger_server.properties file to true.</p>
NGS-24912	<p>The Rest API call getResourceById was failing. This issue has been fixed and the REST API behavior should now be consistent with earlier ESM versions.</p>
NGS-24848	<p>The log file velocity.log is missing in ESM 6.11 due to an update in the third party Velocity library. The velocity logging was updated to work with the new library.</p> <p>Workaround:</p> <p>For logging similar to previous ESM versions, log level must be set to debug in the velocity.properties file.</p>

Issue	Description
NGS-24651	An exception occurred when a user tried to delete 50 assets or more. This issue has been fixed.
NGS-24631	The field Request URL Filename was sometimes blank in reports. This issue has been fixed.
NGS-22565	There were problems with logout tracking for user sessions that were created via REST API. This issue has been fixed.
NGS-22441	Java sort comparison contract changed, causing the following errors appearing in logs when a data structure violated it: java.lang.IllegalArgumentException: Comparison method violates its general contract This issue has been fixed.
NGS-19321	Asset channels did not display location information for automatically-created assets. This issue has been fixed.
NGS-12952	Log messages related to resource name of events forwarded from connectors not registered to a Manager instance are now debug level. To reenable them the Manager side property log.global.debug in server.properties must be set to true.

CORR-Engine

Issue	Description
NGS-27020	The performance of database queries filtered by IP address or IP address range were declined in ESM 6.11. The performance of these queries has been improved.
NGS-26430	Repeated Execute Command rule actions could be significantly delayed. This issue has been fixed.
NGS-23699	When a large number of events are sent to ESM, this may result in a corrupted data chunk due to a BufferUnderflowException and a BufferOverflowException. As a result, some event fields such as Request Url could not be displayed in the ArcSight Command Center and Arcsight Console.

Command Center

Issue	Description
NGS-23154	<p>There is a new feature in the ArcSight Command Center the can require user consent to a banner before login. The banner text is configurable.</p> <p>This feature is enabled with following property in server.properties:</p> <p>auth.login.banner</p> <p>This parameter also activates the Arcsight Console banner.</p>

Connectors

Issue	Description
NGS-26719	<p>Forwarding connectors were not handing the deletion of the user associated with the the connector correctly.</p> <p>The connector was not listening for user deletion events and still trying to process events but throwing exception due to the deleted user. Now, the connector receives a user delete event and shutdowns down.</p>

General

Issue	Description
NGS-27229	<p>Mark similar was creating a configuration instance for each event selected when annotating.</p> <p>Now removing duplicate configuration.</p>
NGS-25006	<p>With existing entry console.ui.imageEditor=true in admin.ast, the "Image Editor" menu entry appeared in the View Menu of the console. But it was not possible to open or edit content in the image editor.</p> <p>This issue has been fixed.</p>

Installation and Upgrade

Issue	Description
NGS-27099	<p>The ESM 6.11.0 Manager was not able to start due to certain certificate attributes becoming unsupported in a third party library update.</p> <p>This issue has been fixed.</p>

Open Issues

This release contains the following open issues.

- [Command Center](#) 25

Command Center

Issue	Description
NGS-27396	The marketplace link for Web Tools Commands is out of date. The correct url is: https://marketplace.microfocus.com/arcshint/content/tool-commands-web-app .

Open and Closed Issues in ESM 6.11.0 Patch 1

For information about open and closed issues for ESM 6.11.0 Patch 1, see the release notes for that release.

Send Documentation Feedback

If you have comments about this document, you can [contact the documentation team](#) by email. If an email client is configured on this system, click the link above and an email window opens with the following information in the subject line:

Feedback on Release Notes (ESM 6.11.0 Patch 2)

Just add your feedback to the email and click send.

If no email client is available, copy the information above to a new message in a web mail client, and send your feedback to arc-doc@hpe.com.

We appreciate your feedback!